

Chapter 8

Privacy and Security

Learning Objectives

At the conclusion of this chapter, the reader will be able to:

- Define and implement organizational policies and procedures to ensure confidentiality, privacy, security, availability and integrity of data
- Assess and mitigate privacy and security vulnerabilities
- Define and implement user access controls according to established policies and procedures
- Assess and implement physical, technical and administrative controls to ensure safeguards are in place to protect assets (e.g., servers secured, unattended computers, two-factor authentication)
- Define organizational roles responsible for managing vulnerabilities (e.g., information security, physical security, compliance)
- Develop and implement data management controls (e.g., data ownership, criticality, security levels, protection controls, retention and destruction requirements, access controls)
- Validate on an ongoing basis the security features of existing systems

Introduction

Concerns about privacy and security of health records are not new to this age of electronic health records (EHRs). In the days of paper records, patients had valid concerns about the privacy of their health information. They expected access to those records would be limited and their contents would remain confidential. What has changed in the era of EHRs is the ease with which health

records could potentially be lost or breached, even from great distances, and the potential scale of these incidents.

Patients have the right to have their health information protected regardless of the form the data is in. Providers are expected to safeguard the patient's health information in order to maintain the patient's privacy rights. The content of a patient's health record is a very valuable asset to the patient and to the provider giving care to the patient. The underlying principle is to do no harm to the patient. Having this health information in a complete and definitive format at the time care is rendered helps the provider make a more informed decision for the patient's plan of care. This formatted health information empowers the patient to be an active member of the care team by having their data readily available to them in many electronic formats and online.

Defining Requirements, Policies and Procedures

Today, numerous laws and regulations exist on international, national and state levels regulating the privacy and security of EHRs. As the use of technologies such as EHRs, personal health records (PHRs), health information exchanges (HIEs) and e-prescribing expands the need for organizations to implement and maintain strong security will continue to be of high importance.

A primary area of focus for many laws and regulations is patient-sensitive health information that is transmitted or maintained in any form or medium. Those rules may impose restrictions on how organizations (including governments in some cases) may use or disclose health information.

In some cases, an individual organization may elect to put in place policies that further restrict access for a variety of reasons, especially when dealing with research that is on the front lines of medical science. For example, the presence in an individual's DNA of a certain genetic marker may not indicate anything today, but as science develops, that same marker could predict a condition that might have negative consequences for the patient.

Health information has been digitized for many decades; however, the Title II Administrative Simplification section of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 established criteria and requirements for a covered entity in the United States to develop and maintain a program to ensure the confidentiality, integrity and availability of this protected health information (PHI). The confidentiality of the data refers to the properties of the information, which render it unavailable such that it cannot be disclosed to unauthorized persons or processes. Integrity is the property that data or information has not been altered or destroyed in an unauthorized manner. Availability means the data is accessible and usable on demand by an authorized person.

This comprehensive HIPAA Administrative Simplification Compliance Program is designed to provide the appropriate policies and procedures to achieve and maintain compliance through internal and external certifications. The

Compliance Program is to be in accordance to the published HIPAA Privacy and Security standards that will position a provider for unannounced inspections by the Office of Civil Rights (OCR), the government entity that will be enforcing compliance of these standards. HIPAA policies and procedures are to address each of the privacy standards and the security standards. Policies define what an organization will do. Procedures define how they will do it. A methodology to achieve and maintain HIPAA compliance can be: project initiation and organization; develop and maintain expertise; provide enterprise awareness and education; establish a baseline assessment of compliance; develop a strategy and compliance plan; remediate gaps in the baseline assessment; implement the program; and have a plan to maintain compliance, effect change control and complete compliance audits.

The HIPAA privacy standards consist of rules for appropriate use and disclosure of patient information; the consent and authorization of these uses; a Notice of Privacy Practices that details how the provider will maintain the privacy of the patient's information; the patient's rights to access, amend, restrict and have an accounting of the flow of their data; training of the provider's workforce members; a patient complaint process; and a process to sanction violators of the policies and procedures plus mitigation so the violation does not happen again. The privacy standards also address any entity the provider contracts with, who is not a provider, but must use the provider's patient information to provide a service. These entities are called business associates and are expected to maintain the confidentiality, integrity and availability of the patient's data in a private and secure manner. This expectation is defined in a business associate agreement with the provider. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 elevated business associates to a level whereby they are held to the same level of accountability as a provider for breaches of privacy and security.

The HIPAA security standards consist of administrative safeguards, physical safeguards and technical safeguards along with organizational requirements. Providers are to have a security program that includes a risk management process, workforce security management, PHI access management and controls, awareness and training, security incident process, contingency plans to protect and ensure uninterrupted access to PHI, facility access controls, workstation use and security, device and media controls, transmission security and business associates agreements. The security standards are classified as either required or addressable. Required standards are to be implemented. Addressable standards are to be documented such that they cannot be reasonably and appropriately implemented and include what can be implemented to meet the intent of the standard. Providers are advised to do an assessment of each standard and document compliance with implementation.

Paramount to having these two programs is to keep them up-to-date, incorporate them into the organizational culture and to do constant surveillance (auditing) to ensure compliance so that the patient has the comfort

level that their PHI is secure, handled with integrity and no breaches have occurred.

The HITECH Act established for the healthcare industry a breach notification process similar to the one used in the financial industry. A breach of this type is the unauthorized acquisition, access, use or disclosure of unsecured PHI that compromises the security or privacy of the PHI. Providers are to provide timely and appropriate notice to affected individuals after a breach has been confirmed and it is believed the PHI has been accessed, acquired or disclosed as a result of such breach. To confirm a breach, a breach notification evaluation can be used. Step one of the evaluation is to determine if the incident involved unsecured information. If there was unsecured information, step two is to determine if there has been an impermissible use or disclosure of PHI under the Privacy Rule. Step three is to determine if the incident falls under one of the exceptions of the breach definition. Step four is to assess the probability that the impermissible use of the PHI would cause harm to the patient. All inappropriate uses of PHI are to be presumed to be a breach unless it can be proven that there is a low probability that the PHI has been compromised. Providers are required to notify the patient of the discovery of a breach without unreasonable delay. For breaches that affect less than 500 individuals, providers are required to enter the breach in an online database with the Centers for Medicare & Medicaid Services (CMS). Providers are required to immediately notify the local media and the Secretary of HHS of any breaches affecting 500 or more individuals.

A prominent international law that includes medical information is the General Data Protection Regulation (GDPR). The GDPR.eu website¹ provides an overview of this regulation. It states that the GDPR is a European Union (EU) law that was implemented on May 25, 2018, and requires organizations to safeguard personal data and uphold the privacy rights of anyone in the EU territory. This regulation includes seven protection and accountability principles of data protection that must be implemented. These principles are:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

This regulation also includes eight privacy rights of the EU people. These rights are:

1. The right to be informed
2. The right of access

3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. the right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Some key GDPR legal terms to be familiar with are:

- Personal data, which is any information about an individual who can be directly or indirectly identified. Personal data can include religious beliefs, web cookies and political opinions.
- Data subject, which is the person whose data is being processed.
- Data controller, who is the person who decides why and how personal data will be processed. This can be a business owner or an employee of the business. Data controllers have to be able to demonstrate they are GDPR compliant.
- Data processor, a third party that processes personal data on behalf of the data controller. The data processor cannot legally process personal data unless they meet one of the following criteria:
 1. The data subject has given consent to the processing of his or her personal data for one or more specific purposes
 2. It is necessary to execute or prepare to enter into a contract
 3. To comply with a legal obligation
 4. To save someone's life
 5. To perform a task in the public interest
 6. There is a legitimate interest to process someone's personal data

Organizations who must be GDPR compliant are to implement appropriate technical measures such as two-factor authentication and end-to-end encryption to handle data securely. Organizations are also expected to implement organizational measures such as staff training, developing a data privacy policy and limiting access to personal data.

The fines for not being GDPR compliant are a maximum penalty of €20 million or 4% of global revenue, whichever is higher. Other sanctions can include a ban on data processing or public reprimands.

HIPAA covers US-based healthcare organizations (covered entities) that handle PHI. The GDPR covers the personally identifiable information (PII) of a EU citizen. This means if a US-based healthcare covered entity uses or stores the PII of a EU citizen this US-based entity must be GDPR compliant regardless of the location of the US-based entity. If there is a breach of this EU citizen's PII, then according to GDPR, the citizen must be informed within 72 hours, where HIPAA has a longer timeframe of notice and a process to evaluate if harm has been done to the patient.

GDPR.eu is co-funded by the Horizon 2020 Framework Programme of the European Union and operated by Proton Technologies AG.

Risk Assessment

Once an organization has developed an awareness and understanding of applicable privacy and security laws and requirements, it should undertake an assessment of the organization's readiness with regard to each of those elements. This assessment should focus on identifying gaps between what is required and what actually exists within the organization's operations. A number of tools may be used in such an assessment.^{2,3} Some examples include:

- Review of current policies, procedures, contracts and other documents relevant to privacy and security
- Organizational surveys or questionnaires that measure knowledge of, and compliance with, applicable privacy and security requirements
- Facility walk-throughs to identify areas where physical security limitations need to be addressed
- Technical penetration or intrusion attempts or other tests to assess security vulnerabilities
- Updated legislation, regulations or international agreements that may drive new approaches
- Root cause analysis of any security breach that may have occurred since the last assessment

This information should serve to give the organization a realistic assessment of its risk. We can think of risk as the likelihood of a given incident occurring, as well as the adverse impact of such an incident. We often think of such risks in terms of threats—potential scenarios that would have a negative impact on security or privacy—and threat sources—persons or events with the ability to actualize a threat. Examples of threat sources include humans (e.g., malicious hackers and employee saboteurs), natural disasters (e.g., floods and earthquakes) and environmental events (e.g., power grid failure and a nuclear or chemical accident). Threats and threat sources are dangerous to any organization that has not made itself entirely immune to them. We use the term *vulnerabilities* to describe flaws or weaknesses that allow exploits or events to result in a security breach or other violation of an organization's security policies.

Risk Management Process

A risk management process includes identifying threats and vulnerabilities, assessing risk and then executing steps to reduce the risk to an acceptable level. A threat is the potential for a thing to go wrong which triggers or exploits a specific vulnerability. A vulnerability is a flaw or a weakness in system components that can result in a breach or violation. Risk is factored by setting a numeric value to the probability a threat will exploit vulnerability and how bad

(criticality numeric value) will the result be. These values are commonly set to HIGH, MEDIUM and LOW on a scale to come to a risk factor. A risk-mitigation process can be used to reduce the risk factor. The process can include what is to be done to reduce the risk, implement controls to reduce the risk and then document the residual risk.

Vulnerability Remediation

The analysis resulting from a risk assessment should go a long way toward identifying the most significant vulnerabilities an organization faces. Additionally, audit reports, reports of atypical system behaviors, vendor advisories and a system security analysis can be used to identify system vulnerabilities. Once those issues have been identified, the organization should embark on a remediation process to eliminate or mitigate the related risks. During the process of remediation, existing policies and procedures will be reviewed, new policies and procedures will be developed, education and training will take place and controls will be put into place to safeguard critical systems and data. The controls include physical safeguards, administrative safeguards and technical safeguards, which will be discussed below. With these tools at its disposal, an organization can decide to take one of two approaches to reduce risk to an acceptable level:

1. No action. The current risk level is deemed acceptable by the organization.
2. Mitigate. Implement safeguards to reduce risk to an acceptable level, along with policies and procedures in support of those safeguards.

User Access Controls

To maintain data confidentiality, integrity and availability, an organization must control access to systems and data. User access controls prevent access by unauthorized users. User access controls can be broken down into the following categories, sometimes termed the AAA or the triple-A approach:⁴

- Authentication
- Access
- Accounting

Authentication is the process of attempting to prove that users are who they say they are before allowing them to access a system. Three primary methods exist to authenticate users:

1. Something a user knows (e.g., personal identification number (PIN) or password)
2. Something a user has (e.g., smart card or token)
3. Something a user is (e.g., fingerprint, palm print or retina scan)

Once a user has been authorized or authenticated, an appropriate level of access must be set. Access privileges are ideally set to allow the minimum access necessary in order to perform a job. Role-based access is often defined by a user's role within the organization. For example, physicians generally have the ability to place orders and to create and sign documents to which a nurse may not have access. A midlevel provider and medical student may each have subsets of the rights granted to a physician, while a pharmacist may have yet another set of privileges in the system.

All authorized users of PHI are to access information systems with a unique user-id. This unique user-id belongs to one person and allows the system to track this user as they do their work to see what data was accessed, modified or deleted. Along with a user-id is the password. Think of the user-id as the key that goes into a door lock. The password allows the key to be turned to open the door. Passwords should have strong characteristics so they are not easily guessed by an unauthorized user or password tracker algorithms. Some of these characteristics of a strong password may include upper and lower case characters, numerical characters, special characters, minimum length, that it cannot match the user-id, is changed periodically and is not reused. User-ids and password should not be written down, stored online, sent to someone in an unsecured e-mail or text and the password should not be sent in the same correspondence as the user-id. Passwords should not be stored on servers or other devices in clear text form. Security criteria set within electronic policies within systems can ensure the rules for user-ids and passwords are followed and not circumvented.

At one time having a password was the effective way to activate a user-id and was very secure; however, advancement of technology and the ease of a program that can be written to crack a password necessitate the need for additional evidence to be entered by the user to further validate who they are. This additional evidence is referred to as two-factor or multi-factor authentication and is known as strong authentication. This additional evidence can be a randomly generated code sent to a mobile device, a PIN, a smartcard, a digital certificate, or a biometric. The goal is to identify and validate the user entering the authentication credentials is the one authorized to use the system. Accounting is the final piece of the user access puzzle. Audit reports and other controls will provide assurance that users are not overstepping their bounds by accessing information that is not required for care delivery and may be forbidden by many privacy laws (e.g., looking up coworkers, neighbors, or celebrities in the system). Audit reports should be generated on both a scheduled and a random basis to ensure ongoing compliance.

Confidentiality, Integrity and Availability

A primary focus of healthcare information technology (IT) security is the area of confidentiality. Confidentiality is the process of limiting disclosure of a patient's personal information to comply with policies and regulations, and to maintain the trust that patients have placed in healthcare organizations.⁵ Two other areas that concern healthcare security professionals are integrity

and availability of data. Integrity refers to the accuracy and completeness of data. To preserve the integrity of its health information, an organization must successfully implement policies and procedures to protect the data from unauthorized modification, deletion or destruction and to keep it consistent with its source. Additionally, the organization must provide auditing mechanisms to ensure data has not been altered, deleted or destroyed in an unauthorized manner. Availability calls for information to be protected from any unplanned destruction, whether by accident, vandalism, natural disasters and so on. Availability also makes certain health information is available to patients when they need it. Care must be taken to ensure that records will be available and survive the organization in the event of closure, merger or similar events. This could also apply to other countries and their internal and external ties through treaties and the like.

Organizational Roles

An expert who understands which privacy laws apply to an organization and how they should be properly interpreted plays a crucial role in most healthcare organizations. Laws in many jurisdictions require that each organization appoint an individual, sometimes with the title of chief information security officer, who is tasked with these responsibilities. Among this individual's tasks will be:

- Assessing and maintaining knowledge of rules and regulations
- Developing policies and procedures
- Cultivating organizational and cultural awareness and developing educational plans in support of policies
- Managing appropriate access for external business partners and ensuring documentation exists in support of such access
- Monitoring compliance with policies
- Responding to complaints and other issues that arise
- Conducting or directing others to conduct scheduled and random access audits
- Investigating known security breaches and reporting information to appropriate regulatory or governmental agencies as required by law

The privacy standards require the provider to identify a position who will be responsible for the privacy program. The security standards have the same requirement and this person is responsible to ensure the security standards are consistently met. These individuals are commonly referred to as the privacy officer or the security officer. They can be two distinct people or they can be the same person. This person(s) is to be responsible for the development, maintenance and adherence to all policies and procedures needed for the provider to be HIPAA compliant.

An important process the privacy officer and/or security officer can oversee is the security incident management process. All incidents, threats or violations that affect or may affect the confidentiality, integrity, or availability of confidential information are to be reported and responded to in accordance to policy and procedure. The officers can oversee these processes and take steps to mitigate so the incidents will not be repeated in the future.

Data Management Controls

To ensure the security of protected data, a number of safeguards may be deployed. These safeguards seek to meet certain goals, including controlling electronic access to systems containing sensitive patient information or other private data; controlling physical access to locations or devices that may have ready access to secure data; managing data in transit, including e-mail and file transfer; and encryption of data on laptop computers, flash memory drives, or other devices that might be easily lost or stolen.

Safeguards can be categorized into three main groupings: administrative, technical and physical. Administrative safeguards are administrative actions, policies and procedures that an organization deploys in support of its security aims. Administrative safeguards include such actions as the ongoing education of employees on security requirements and scenarios in which data may or may not be used or disclosed, as well as developing policies and procedures that provide safeguards within the physical and technical realms.

Technical safeguards are electronic means of ensuring that data is not accessible, or that it is encrypted in a way that makes it useless to a third party. Examples of technical safeguards would include the use of network firewalls, secure protocols on any public networks carrying patient data and encryption of storage media on laptop computers and mobile devices.

The last type of measure, physical safeguards, consists of physical measures, policies and procedures that protect electronic information systems from natural and environmental hazards, as well as unauthorized intrusion. Examples would include data centers that are located outside a floodplain and have redundant sources of power, and limited access to server rooms or areas where data may be accessed or damaged. One of the major threats security professionals face today is cybersecurity—or the unauthorized access and malicious attack of healthcare information systems and patient health information data and more recently, ransomware—holding that patient health information “hostage” for payment.⁶

A data classification policy can be designed to support the minimum amount of data needed by a user to do their job. This ensures the information will be protected from unauthorized disclosure, use, modification and deletion. This policy is applicable to data is created, received, stored and/or maintained by the

provider. This data is to be consistently protected throughout its life cycle, from origination to its destruction. Data will be protected in a manner commensurate with its sensitivity, regardless of where it resides, what form it takes, what technology was used to handle it and what purpose(s) it serves. Common data classifications are Public, For Internal Use Only, Confidential and Restricted Confidential. A data classification matrix can be developed to document for each classification examples, criteria, handling standards, copying standards, storage standards, destruction standards and workforce classification and access availability.

The volume of data being created, maintained, received, stored and transmitted by healthcare providers is enormous. Data management is necessary to ensure the most useful data is quickly available. Providers are advised to develop a data retention and destruction policy and procedure so non-useful data or data that has reached its end of life can be systematically destroyed. Destruction schedules can be developed to define the data and define the timeframes for destruction based on workflow process needs, regulatory reporting, state regulations, or federal regulations. The data owners (those who generate and maintain the data) can be the party to define the content of the destruction schedules. Review of these schedules should be done on a routine basis to stay abreast of any recent regulatory changes.

Disaster Recovery and Business Continuity Plans

While everyone has responsibility for protecting patient privacy and ensuring healthcare data security, the healthcare IT security professionals must be involved in the development of an organization's disaster recovery and business continuity plans. Contingency plans in this area should include the following:

- Analysis of applications and data criticality. Applications and data should be prioritized in order of importance to the organization so a logical sequence of data recovery can be planned
- Data backup plan. Detailed plans must be developed to ensure the existence of a retrievable backup copy of the organization's critical data
- Disaster recovery plan. Procedures must be documented that define how to restore data after any loss, for any reason
- Emergency-mode operation plan. Downtime plans should be spelled out that will enable the organization to continue to operate in emergency mode while access to electronic data is not possible
- Testing and revision. All contingency plans must be routinely tested and revised to fill gaps that are discovered and to address changing organizational needs and infrastructure

Auditing

An essential component of an organization's security plans is the ability to audit all access to protected data. No matter how good an organization's policies and procedures are or how strenuously it works to limit access, individuals may still be able to access records they may not need to access to perform their daily duties. Audit reports enable an organization to identify any breaches or other policy violations, from employee snooping to a large criminal attack.

Validation of consistent compliance with the HIPAA security standards is a structured security audit program and risk-assessment process for any changes made to security features of all systems in the providers' IT environment. These audits can be done internally or externally by a third party. Industry standard is to have an objective third party conduct annual external network penetration testing from outside the provider's network to identify vulnerabilities in the network perimeter that would allow unauthorized individuals to access the provider's core network infrastructure and render the network inoperable. This same testing can include an internal network vulnerability assessment, a wireless network assessment, medical devices assessment, social engineering and a firewall rules review. The findings from the third-party assessment can then be incorporated into the provider's risk-assessment process to document a starting risk, mitigation, controls and residual risk in order to show security features are being maintained at the highest level of integrity.

Ongoing System Evaluation

Ensuring security is an ongoing and critical process. Crucial to maintaining compliance is a continuous evaluation of the security features of existing and new hardware and software. Network diagrams that include the location and configuration of firewalls, servers and routers must be maintained. Documentation of software and hardware, as well as vendor contact information, must be kept up-to-date. As new applications are introduced, technical and user interfaces and other data access points must be evaluated and care must be taken to assess whether an application or interface might introduce new security vulnerabilities. Additionally, existing applications must be reevaluated on an ongoing and regular basis in the face of organizational changes and evolving local, national and international attitudes, laws and regulations.

Summary

Ensuring the privacy and security, while also guaranteeing the confidentiality, integrity and availability of health information, is an ongoing and critical process. The introduction of EHRs has also shifted the landscape of what

maintaining and protecting a patient's record looks like. New policies and procedures, new laws and regulations and new personnel and workforce focused on these important tasks have grown significantly over recent years. It is important that organizations focus on privacy and security on a consistent basis. It is not something that should be periodically "checked-in" on. Compliance programs must be in place, audits should be conducted regularly, data management controls and safeguards, administrative, technical and physical, should be in place, risk assessments that identify vulnerabilities should be occurring regularly, with mitigation plans enacted, disaster recovery and business continuity plans should be documented and contingency planning should be a continuous focus. And, although there are organization roles that are primarily responsible for this, health information privacy and security is everyone's responsibility.

References

1. Complete Guide to GDPR Compliance. <https://gdpr.eu> (accessed September 6, 2019).
2. ONC (Office of the National Coordinator for Health Information Technology). Security Risk Assessment Tool. Washington, DC: ONC. <https://www.healthit.gov/providers-professionals/security-risk-assessment-tool> (accessed November 10, 2015).
3. HIMSS (Healthcare Information and Management Systems Society). Risk Assessment Toolkit. Chicago: HIMSS. <http://www.himss.org/library/healthcare-privacy-security/risk-assessment> (accessed November 10, 2015).
4. Newman RC. Computer Security: Protecting Digital Resources. Sudbury, MA: Jones and Bartlett, 2010.
5. HIMSS (Healthcare Information and Management Systems Society). Privacy & Security Toolkit. Chicago: HIMSS, 2013. <http://www.himss.org/library/healthcare-privacy-security/toolkit> (accessed November 10, 2015).
6. HIMSS (Healthcare Information and Management Systems Society). 2015 HIMSS Cybersecurity Survey. Chicago: HIMSS, 2015. <http://www.himss.org/2015-cybersecurity-survey> (accessed November 10, 2015).